Department of Information Technology

Y2K INFORMATION TECHNOLOGY DIRECTIVE

NUMBER: 1999-11	
SUBJECT: Y2K and Security – Bridging the Gap	**DATE ISSUED**: December 6, 1999
REFERENCES: Governor's Executive Order D-3-99	**SUPERSEDES**:

To: Agency Secretaries
Department Directors
Chief Information Officers
Y2K Project Managers
Information Security Officers

From: DEPARTMENT OF INFORMATION TECHNOLOGY

In an effort to increase the awareness and knowledge of the State's Information Technology (IT) professionals, the Department of Information Technology (DOIT) and the Governor's Office of Emergency Services (OES) have arranged to provide Year 2000 (Y2K) Security Training Seminars. The five, half-day sessions will be held at the **Sacramento Convention Center** on **December 14, 15 and 16.** This training is free of charge to all attendees.

Y2K Security topics of discussion and planning include:

- Information Assurance
- Incident Handling and Response and Disaster Recovery
- NT Security – Oxymoron?
- UNIX/Linux Security
- Technologies, Trends and Threats

Attendance of IT professionals at the first session, Information Assurance, is mandatory. Additionally, we strongly encourage you to send the appropriate staff (e.g., Database Administrators, Web and Network Administrators) to attend as many sessions as is relevant to your organization. The attached agenda and registration form provide more details about the actual seminars.

Please register by Thursday, December 9, 1999. If you have any questions about this directive, please contact Lance Williams, DOIT, at (916) 445-7020.

JEFFREY R. PELL
Year 2000 Program Director
Department of Information Technology

Attachments: Agenda
Registration Form

DEPARTMENT OF INFORMATION TECHNOLOGY
and the
GOVERNOR'S OFFICE OF EMERGENCY SERVICES

AGENDA

Y2K Security Training Seminar

Sacramento Convention Center

Room 314

DATE				
Tuesday, December 14		**Wednesday, December 15**		**Thursday, December 16**
Session 1 – Information Assurance	**Session 2 – Incident Handling and Response**	**Session 3 – NT Security – Oxymoron?**	**Session 4 – UNIX/Linux Security**	**Session 5 – Technologies, Trends and Threats**
Registration: 8:00 AM Conference: 9:00 AM - 11:45 AM	Registration: 12:00 PM Conference: 1:00 PM - 3:45 PM	Registration: 8:00 AM Conference: 9:00 AM - 11:45 AM	Registration: 12:00 PM Conference: 1:00 PM - 3:45 PM	Registration: 8:00 AM Conference: 9:00 AM - 11:45 AM
Introductions and Overview Objectives What is Information Security? Physical, Logical, and Human Factor The Need for Security Security Model Totality of Security Who are we Protecting Ourselves Against? Security Policy Authenticity vs. Masquerading Privacy vs. Interception Integrity vs. Modification Availability vs. Interruption Common Attack Methods PIE – Personal, Interior, and Exterior Attack Countermeasures SATE – Security Awareness, Training, and Education Threats (Special Focus on Viruses) • What are viruses? • How Viruses Affect (and infect) your system • What should you do to protect your system? • Implications for System Administrators • Special Section: • Macro Viruses • What Is a Macro Virus? • How Do Viruses Spread? • How Do You Prevent the Spread of Viruses? • How to turn on MS-Word Protection Suggested Actions	Introductions and Overview Objectives What is an Incident? Preparing for Incidents "Five P's" Planning, Notification, Assessment, Handling, Aftermath, and Responsibility Points of Contact and Responsibility Identifying an Incident Dealing with the Incident After the Incident Y2K Y2K Transition Suggested Actions	Introductions and Overview Objectives Brief Microsoft Windows NT History NT Security Checklist Phase 1-Setting up the Machine Phase 2-Setting up a Safe File System and Creating an Emergency Repair Disk Phase 3-Setting Registry Keys Phase 4-Establishing Strong Password Controls and Secure Account Policies Phase 5-Auditing Phase 6-Networking & Internet Security Settings Phase 7-Other Actions Required as the System is Setup Phase 8-Monitoring and Updating Security and Responding to Incidents NT and Y2K Three steps to ensuring Y2K compliance for Windows NT 4.0 Suggested Actions	Introductions and Overview Objectives UNIX Checklist Patches Network security ftpd and anonymous ftp Password and account security File system security Vendor operating system specific security Security and the X Window System Linux Checklist UNIX/Linux and Y2K SuSE, Debian, and Caldera Suggested Actions	Introductions and Overview Objectives Past, Present, and Future Emerging Technologies: • PKI • Firewall • IPSec • VPN's • Biometrics Cryptography Trends: (Special Focus on Y2K) • Y2K • History of the problem • The Current Problem • The Leap Year Problem • Y2K CHECKLIST Suggested Actions

DEPARTMENT OF INFORMATION TECHNOLOGY
and the
GOVERNOR'S OFFICE OF EMERGENCY SERVICES

YEAR 2000 SECURITY TRAINING SEMINAR

TRAINING REGISTRATION

Please Register by E-mail or by Fax
E-mail: Lance.Williams@doit.ca.gov FAX: (916) 445-6524

For Information Call
(916) 445-7020

PARTICIPANT INFORMATION

Agency/Department/County Name

Agency/Department/County Address – Number, Street City State Zip

Please list the names of the people who will be attending and indicate which session(s) they will be attending.

	Name	Job Title	Phone Number	Fax Number	E-Mail Address	Session # (✓)				
						1	2	3	4	5
1										
2										
3										
4										
5										
6										
7										
8										

***** Please register no later than Thursday, December 9, 1999. *****
You are encouraged to register as early as possible.